AlliedWare Plus Software Maintenance Release Note

Software Version 5.3.2-0.2 For SwitchBlade x908, x900-12XT/S, x900-24 Series, and x600 Series Switches

Introduction

This release note lists the issues addressed and enhancements made in AlliedWare Plus software maintenance version 5.3.2-0.2. Version details are listed in the following table:

Models	Series	Release File	Date	GUI file
x600-24Ts, x600-24Ts/XP, x600-48Ts, x600-48Ts/XP	x600	r6-5.3.2-0.2.rel	27 August 2009	gui_532_20.jar
SwitchBlade x908	SwitchBlade	r1-5.3.2-0.2.rel	27 August 2009	gui_532_20.jar
x900-12XT/S, x900-24	x900	r1-5.3.2-0.2.rel	27 August 2009	gui_532_20.jar

Caution:
Information in this document is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

The issues addressed in this document include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

Level 1 This issue will cause significant interruption to network services, and there is no work-around.

Level 2 This issue will cause interruption to network service, however there is a work-around.

Level 3 This issue will seldom appear, and will cause minor inconvenience.

Level 4 This issue represents a cosmetic change and does not affect network operation.

Installing and enabling this version

To use this maintenance version, your switch must already be running AlliedWare Plus. Contact your distributor or reseller for more information.

To install this maintenance version, use the following steps:

1. Put the maintenance version file onto your TFTP server.
2. If necessary, delete or move files to create space in the switch's Flash memory for the new file.

   Note that you cannot delete the current boot file.

   To list files, use the command:

   ```
   awplus#dir
   ```

   To see the memory usage, use the command:

   ```
   awplus#show file systems
   ```

   To delete files, use the command:

   ```
   awplus#del <filename>
   ```
3. Copy the new release from your TFTP server onto the switch.

   To do this, enter Privileged Exec mode and use the command:

   ```
   awplus#copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.
4. Set the switch to boot from the new release.

   To do this, enter Global Configuration mode and use the command:

   ```
   awplus(config)#boot system r1-5.3.2-0.2.rel
   ```

   If desired, check the boot settings by entering Privileged Exec mode and using the following command:

   ```
   awplus#show boot
   ```
5. Reboot.

   To do this, enter Privileged Exec mode and use the command:

   ```
   awplus#reload
   ```

Features in 5.3.2-0.2

AlliedWare Plus maintenance version 5.3.2-0.2 includes the resolved issues in the following tables.

Level 1

No level 1 issues.

Level 2

CR	Module	Level	Description
CR00026531	**Core**	**2**	Previously, the switch could stop routing and fail to recover under low free memory conditons. This issue has been resolved. Memory usage is now maintained at a level which prevents this problem.

CR00026725	**VCStack**	**2**	File directory corruption could happen when doing a file **copy** from a stack backup member to a TFTP server without specifying a source file name in the command.
			This issue has now been resolved. Now, Users will be prompted to enter a source file name if it is not specified in the command. Wild card use is allowed.
			For example:
			`awplus#copy backupmember/flash: tftp  <--- no file name is specified`
			`Enter source file name []:myfile.cfg  <---- prompt user to give one`
			`Enter destination host name []:172.16.138.1`
			`Enter destination file name [myfile.cfg]:`
			`Copying..`
			`Successful operation`
			`awplus#`

CR00026539	**How Swap**	**2**	There was some loss of multicast traffic (about 27%) after hotswapping a XEM that had static-channel ports configured. This issue has been resolved.
CR00026605	**DHCPv4**	**2**	When a secondary IP address was configured on any interface, enabling DHCP server caused the switch to undergo a system reboot. This issue has been resolved.
CR00026611	**SFP**	**2**	1) Inserting a AT-SPFX/2 SFP could cause all future SFP status changes (Insertion/ Removal/ Fault) to be missed. 2) If the **shutdown** command was run on a port containing an AT SPFX/2 SFP the LED would display a fault. 3) When hot swapping out a XEM-12S with certain SFPs in a x908, the switch could lock up and undergo a system reboot after 3 minutes. These issues have been resolved.
CR00026616	**ARP**	**2**	On the x600 when a MAC/VLAN entry moved between ports, ARP entries associated with the MAC/VLAN entry were not updated. This issue has been resolved.

CR	Module	Level	Description
CR00026658	**VRRP**	**2**	Occassionally, hosts were unreachable on a VRRP interface when the switch transitioned to its Master, due to static routes being removed from the routing table. This issue has been resolved.
CR00026695	**PIM**	**2**	Previously if multicast groups existed in the presence of a 6to4 tunnel, then the multicast traffic may not recover in some instances. This issue has been resolved.
CR00026724	**EPSR**	**2**	With r1-5.3.2-0.1.VCStack fail over could cause an EPSR ring to storm if many data VLANS were configured on the switch. This issue has been resolved.
CR00026731	**DHCP**	**2**	Previously, and imi core dump could occur when configuring DHCP -server. Any of the following could result in IMI exiting, a core dump being generated, and the user being prompted to login again: 1) "ip dhcp option <option number> name <option name> <type>" where <option name> is longer than approx **80** characters. 2) "ip dhcp pool <pool name>" where <pool name> is longer than approx **80** characters, then setting the pool's network with "network <network addr>" 3) "host <IP addr> <MAC addr>" when pool's network is set. 4) "bootfile <filename>" where <filename> is longer than approx **80** characters and the pool's network is set. 5) "domain-name <domain name>" where <domain name> is longer than approx **80** characters and the pool's network is set. 6) "option <option name> <value>" where <value> is longer than approx **80** characters and the pool's network is set. These issues have now been resolved [NOTE: Although this issue has not been seen on any existing releases (i.e. 521, 522, 531, or 532) there is still potential for it to occur in any of these under some circumstances.]
CR00026773	**IGMP Snooping**	**2**	When a switch was configured for PIM, in some circumstances it could fail to also L2 switch streams. This was because disabling then re-enabling IGMPSnooping report suppression on an interface was causing IGMP and IGMPSnooping on the interface to be put in an inactive state. This issue has been resolved.
CR00026775	**IGMP**	**2**	Previously, IGMP snooping failed to stop L2 multicast data flow on to ports with expired group membership. This issue has been resolved.
CR00026785	**PIM**	**2**	It was possible in certain PIM-DM networks that two switches connected at Layer 2 and Layer 3 would not complete the Assert process correctly. This issue has been resolved.
CR00026792	**VCStack**	**2**	When a stack of x900 or x908 devices were booted up, the switch's MAC address were sometimes not added to hardware for the default VLAN on the backup member. This meant that any packets unicast to the switch on VLAN 1 and ingressing on the backup member would not be received. This issue has been resolved.

CR	Module	Level	Description
CR00026816	**BGPv4**	**2**	When entering the command **neighbor [addr] interface [int]** in BGP router configuration mode, if the interface being referenced did not have an IP address configured, BGP would restart. This issue has been resolved.
CR00026831	**802.1x**	**2**	When a port was in multi-host mode and it was already in authorized status, then authentication requests from later supplications removed the dynamically assigned VLAN information on the port. This issue has been resolved.
CR00026878	**IGMP Snooping**	**2**	With Global IGMP Snooping disabled in the configuration if the switch was restarted, IGMP packets were not being flooded out of VLANs other than VLAN 1. This issue has been resolved.
CR00026900	**IGMP Snooping**	**2**	If the port in a Layer 2 multicast network on which IGMP reports were being received was taken down and brought back up and the reports were sent again, multicast traffic was not getting forwarded to the port. This issue has been resolved.
CR00026957	**EPSR**	**2**	Previously, multicast traffic in an EPSR environment could cause very high CPU usage on one or more of the devices in the ring. This has been corrected, and CPU usage due to MAC learning should be limited to approximately 25%.
CR00026997	**LLDP**	**2**	When the switchreceived an updated LLDPDU from a neighbor that contained *new* information, a small amount of memory would be lost. If a large amount of such updates were received, the LLDP process could eventually run out of memory and be restarted. This would not normally occur in a stable network. This issue has been resolved.
CR00027010	**OSPF**	**2**	If OSPF was configured to redistribute static routes, and it also received those routes as LSA type 5 updates from another OSPF router, it would create unnecessary route entries that would consume memory as well as count towards the route licensing limit for OSPF (eg, 64 route cap) each time an LSA update was received. This would eventually leave OSPF in a state where it could no longer learn new or updated routes of any type from other OSPF routers, as indicated by the following message appearing in the log: "OSPF[1094]: RT[Install] Licence: route limit breached: limit=64, breach=1, watermark=1" This issue has been resolved. - OSPF will now only create a single route entry for each LSA type 5 entry received in this scenario.
CR00027032	**LACP**	**2**	When the link on a port that is a member of an aggregator changed debug messages were sent to the log. These messages have been suppressed and won't appear in the log unless enabled by an ATI support engineer. This issue has been resolved.
CR00027084	**HSL**	**2**	Previously, on an x600 switch, if a stacking cable was not screwed in correctly it could cause many link up/down events, which could cause a system reboot in the switch if too many events arrived too quickly. This issue has been resolved.

CR	Module	Level	Description
CR00027107	**IGMP**	**2**	On a Layer 3 multiple VLAN multicast switch, mutlicast traffic was not being switched to other VLANs when IGMP v1 or V2 reports were received on the receiving VLANs that were receiving the multicast streams. This issue has been resolved.
CR00026421	**MSTP**	**2**	Query solicitation was not working properly with MSTP, with Query solicit packets not getting sent as part of Topology change. This issue has been resolved.
CR00026577	**VRRP**	**2**	If VRRP was configured on a switch, the virtual MAC address was being used for both the virtual IP and the switches own IP. This issue has been resolved. Now the switches MAC address is used for its own IP address (if different from the virtual IP).
CR00026763	**EPSR**	**2**	Previously, a link down event followed quickly by a link up could cause a storm in an EPSR ring, if the master was under load. This issue has been resolved. Now, Enhanced recovery mode must be turned on in order to recover from a second link failure immediately after the first link failure has recovered, which was not required in the past.
CR00026777	**Hot Swap**	**2**	Previously, when multicast traffic was running through a switch and the XEM that contained a port connected to the multicast source was hotswapped, a system reboot could occur. This issue has been resolved.
CR00026983	**PIM**	**2**	Previously, if there was an MSTP topology change, this could cause a switch running PIM to have a system reboot. This issue has been resolved.
CR00027165	**VCStack**	**2**	Under certain circumstance, after a master failover, ports would not be added back to the Static Aggregator. This issue has been resolved.
CR00027166	**IPv6**	**2**	Previously, if a 6to4 tunnel end-point decapsulated IPv6 packets with destination address not matching any other routes except the 2002::/16 routes, it would consume large amounts of memory. This issue has been resolved.
CR00027167	**MLD**	**2**	Previously, ports on which IPv6 Router Advertisements had been received, were not being learned as Router ports. This stopped MLD packets being forwarded out of these ports. This issue has been resolved.
CR00027242	**VCStack**	**2**	Traffic to the CPU received on a XEM-1XP in a VCStack was, sometimes not fully processed by the CPU. This issue has been resolved.
CR00026546	**VLAN**	**2**	When a VLAN was deleted, ports using that VLAN as native VLAN were not set back to use the default native VLAN. This issue has been resolved.
CR00027060	**ACL** **QoS**	**2**	Previously the SBx908 only allowed adding 1248 access lists per XEM regardless of the routing ratio setting. This issue has been resolved. Now if the routing ratio is unset or is set to IPv4 only, 2048 access lists can be added per XEM. If the routing ratio is set to IPv4 and IPv6 the limit of 1248 remains.

CR	Module	Level	Description
CR00027275	PIM -SM	2	Previously on an x600 as a transit node in an EPSR ring running PIM-SM, if there was a break of the EPSR primary, it could result in loss of traffic. This issue has been resolved.
CR00027295	VCStack	2	XFPs would link up if they were shutdown by the boot config. No traffic would be passed but the LED would show the port as being up and the remote end would think the link was up. This didn't occur if the port was manually shut down from the CLI. This issue has been resolved.
CR00027349	Telnet	2	Previously, some commands that could take more than one user argument, could fail to execute after a delete command was entered. This issue has been resolved.
CR00027366	VCStack	2	When a unit in a stack x600s' lost it's stack connections but resiliency links were in place, the secondary master could sometimes form as an active master instead of a disabled master. This issue has been resolved.

Level 3

CR	Module	Level	Description
CR00025784	CPU	3	Previously whenever a minute average CPU reached 100%, in the 30 minutes CPU usage graph, the spike would stay there and never rolled out of the time window. This issue has been resolved. Now, the spike high appears in the graph when the 1min average is actually 100%, but it will roll out along time passing and disappear when the time window rolls over.
CR00021918	SFP	3	A new command **show system pluggable detail** has been created to display further information on SFP modules. The extra information includes the SFP wavelength and some length properties (single mode fiber, OM2 fiber and OM1 fiber). For further information, please see:**"Show System Pluggable Detail (CR00021918)" on page 11**
CR00022140	VCStack	3	On a VCStack, if the **boot system** command was aborted by entering CTRL+C, then the CLI prompt would continue to display the command progress (indicated by periodically displaying '.' dots) indefinitely. This issue has been resolved.
CR00025582	Log	3	There was a 'Name or service not known' message in the log when the switch booted. This issue has been resolved, now there are no such error messages in the log.

CR	Module	Level	Description
CR00025648	**LLDP**	**3**	Previously, VLAN names stored in LLDP could become corrupted. This occurred when the names had been changed from their default values and command line operations had been performed on ranges of VLANS, e.g. **vlan 25-30 state enable**. This impacted the names displayed in the **show lldp local-info** output and in the LLDP PDUs. This issue has been resolved.
CR00025651	**LLDP**	**3**	Previously, LLDP could be configured to transmit LLDPDUs out ports configured as VCS resiliency link ports. This issue has been resolved. - LLDP is now always completely inactive on such ports. Also the **show lldp interface** command output now indicates any ports that are configured as mirror analyser ports, and therefore not available for LLDP.
CR00025702	**LLDP**	**3**	Previously, dynamic VLAN information was not being synchronized to LLDPD after the switch restarted. This issue has been resolved.
CR00025996	**Triggers**	**3**	When a trigger was activiated with multiple scripts configured, the scripts were being executed in parallel. This issue has been resolved, now scripts are executed in the order specified.
CR00026151	**LLDP**	**3**	When the switch sent LLDP traps, the remote table sometimes changed the SNMP notification for LLDP to an incorrect ASN type. This issue has been resolved. Now, the SNMP notification for LLDP has been corrected to ASN_GAUGE.
CR00026234	**LLDP**	**3**	Previously, when LLDPD restarted, an interface was not made available for LLDP if the port was a member of a channel group. This issue has been resolved.
CR00026378	**ARP**	**3**	If a loop was configured in the network, a storm of ARP packets could delay MAC thrash detection and stop its action from occurring. This issue has been resolved.
CR00026402	**SSL**	**3**	The **crypto pki enroll local user** command wasn't rejecting user names that included unuseable characters. This issue has been resolved. Now the following commands can use alphanumeric and ! % , = @ ~ _ { }. - **crypto pki enroll local user** **- no crypto pki enroll local user** **- crypto pki enroll local local-radius-all-users** **- show crypto pki certificate user** **- crypto pki export local pkcs12**
CR00026524	**SNMP MIB Support**	**3**	Previously, addition of duplicate NTP peers and server via SNMP would be allowed. This was incorrect and has been resolved. Now no duplication will be allowed.
CR00026646	**CLI**	**3**	The **no thrash-limiting** command was not able to be configured on an aggregator interface. This issue has been resolved.

CR	Module	Level	Description
CR00026687	**LLDP**	**3**	Previously, LLDP was being disabled on interfaces by default for transmit and receive and two commands were required to enable LLDP on an interface: l**lldp run** and **lldp receive transmi**t. This issue has been resolved. Now the default settings for LLDP transmit and receive on an interface is **enabled by default**.
CR00026721	**VCStack**	**3**	Previously, the Loop Detection Feature (LDF) didn't work after a VCS failover occured.The cause of this problem was that the hardware table entries for LoopProtection awere not synchronized to the new backup member. The new backup member would not detect reception of the LDF packet, so the loop protection did not work correctly. (Note: This issue occurred only on x900 series switches) This issue has been resolved.
CR00026736	**LLDP**	**3**	Neighbour entries were not clearing after the **no lldp run** command entered. This issue has been resolved. When disabling LLDP using **no lldp run**, all entries in the neighbour table are now automatically cleared.
CR00026860	**LLDP**	**3**	LLDP would not properly display non-ascii characters in textual TLV strings received from neighbor devices. This issue has been resolved. Now, if any such characters are received in a textual TLV string the hex value of the character will be displayed in the form \x06.
CR00026871	**LLDP**	**3**	When multiple identical bad LLDP PDUs were received from a particular neighbor, global error counters would not be incremented for each bad PDU after the initial one. This issue has been resolved.
CR00026692	**VLAN**	**3**	Previously, a VLAN range in the switches running-config was not incorrectly formatted, so MLD snooping did not always apply to the first 100 available VLANs. This issue has been resolved.
CR00026750	**VLAN**	**3**	If a subnet based VLAN classifier was configured on a backup member's port, ARP packets were sometimes not handled correctly. This issue has been resolved.
CR00027163	**NSM**	**3**	Receiving an invalid IGMP packet could cause a system reboot. This issue has been resolved.
CR00027231	**Port Auth**	**3**	When using the commands **supplicant-mac** and **disable auth-mac**, sometimes a system reboot could occur, or the authentication feature did not work. This issue has been resolved.
CR00027201	**DHCP**	**3**	Previously, if the DHCP directory in NVS was deleted it would not be recreated. This issue has been resolved.

Level 4

CR00024929	**TFTP**	**4**	Previously, the filename specified in a TFTP read request packet sent by AlliedWare Plus had an forward slash, '/', prepended to the start of the name. Some TFTP servers will reject such a read request. The operation of TFTP has now been changed, so that there is no longer a forward slash prepended to the filename in the read request packet.
CR00025432	**Log**	**4**	Previously, on AllliedWare Plus software version builds, the host name in the **send syslog message** was displayed as [HOSTNAME]. Now, the host name of the send syslog message has the characters s_src@ appended before the hostname, for example: s_src@[HOSTNAME].
CR00025638	**LLDP**	**4**	Previously, time values in the output of the **show lldp** command were displaying the seconds units incorrectly. This issue has been resolved and the command now shows reinit delay and tx delay with units of "sec" if value is 1, and "secs" otherwise.
CR00026588	**SSL**	**4**	When the command **exit** is issued while in ca-trustpoint mode, it is now moved to config-mode.

Enhancements

CR	Module	Description
CR00026556	**VRRP**	This maintenance release adds the commands **undebug all** and **no debug all** to support VRRP, so that VRRP debug messages can now be stopped by those commands. A VRRP filter has also been added to these commands. The **no debug all** command disables the debugging facility for all features on the switch. This stops the device from generating any diagnostic debugging messages. The debugging facility is disabled by **default**. The command is available in Global Configuration mode and Privileged Exec mode.

CR00026749	**TFTP**	Previously, copying a file into startup-config via TFTP was not supported. This feature has been implemented.
		The following command is now valid:
		`awplus#copy tftp startup-config`
		`Enter source host name []:172.16.138.1`
		`Enter source file name []:epsr.cfg`
		`Copying..`
		`Successful operation`
		`awplus#`
		or
		`awplus#copy tftp://172.16.138.1/epsr.cfg startup-config`
		`Copying..`
		`Successful operation`
		`awplus#`

Show System Pluggable Detail (CR00021918)

This command displays detailed information about the pluggable transceivers, such as SFPs or XFPs, which are currently installed in your switch.

In addition to the information about pluggable transceivers displayed using the **show system pluggable** command (port, manufacturer, serial number, manufacturing datecode, and type information), the show system pluggable detail command displays the following information:

- **Wavelength**: Specifies the laser wavelength of the installed pluggable transceiver
- **Single mode length**: Specifies the link length supported by the pluggable transceiver using single mode fibre
- **OM1 length:** Specifies the link length supported by the pluggable transceiver using 62.5 micron multi-mode fibre.
- **OM2 length**: Specifies the link length supported by the pluggable transceiver using 50 micron multi-mode fibre.

For parameters that are not supported or not specified, a hyphen is displayed instead.

For a stacked configuration, if this command is entered on the stack master, it will display detailed information about the pluggable transceivers for all the stack members. A stack member heading will be displayed to distinguish the different pluggable transceiver information for every stack member.

If it is entered on a specific stack member, as a host-directed command, it will display detailed information about the pluggable transceiver for that stack member.

Syntax

```
show system pluggable detail
```

Mode

Exec mode and Privileged Exec mode

Example

To display detailed information about the pluggable transceivers installed on a standalone switch, use the command:

```
awplus# show system pluggable detail
```

Output

Figure 1: Example output from the **show system pluggable detail** command on a switch

```
System Pluggable Information Detail
Port1.0.45
==========
Vendor Name:              ATI
Device Name:              AT-SPLX10
Device Type:              1000BASE-LX
Serial Number:            0000071004100004
Manufacturing Datecode:   07040900
SFP Laser Wavelength:     1310nm
Link Length Supported
  Single Mode Fiber :     10000m
  OM1 (62.5um) Fiber:     -
  OM2 (50um) Fiber  :     -
```

Example

To display detailed information about the pluggable transceivers installed on a stack, use the command:

```
awplus# show system pluggable detail
```

Output

Figure 2: Example output from the **show system pluggable detail** command on a stack

```
Stack member 1:
Port1.0.45
==========
Vendor Name:              AGILENT
Device Name:              HFCT-5710L
Device Type:              1000BASE-LX
Serial Number:            0402142241184360
Manufacturing Datecode:   040214
SFP Laser Wavelength:     -
Link Length Supported
 Single Mode Fiber :     10Km
 OM1 (62.5um) Fiber:     550m
 OM2 (50um) Fiber  :     550m

Stack member 2:

Port2.0.47
==========
Vendor Name:              FINISAR CORP.
Device Name:              FTRJ-8519-7D-CSC
Device Type:              1000BASE-SX
Serial Number:            P430KGY
Manufacturing Datecode:   030718
SFP Laser Wavelength:     850nm
Link Length Supported
  Single Mode Fiber :     -
  OM1 (62.5um) Fiber:     300m
  OM2 (50um) Fiber  :     550m
```

Related Commands

show system environment
show system pluggable